

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- [High](#) - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- [Medium](#) - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- [Low](#) - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Amazing Flash Commerce -- AFCommerce Shopping Cart	SQL injection vulnerability in Amazing Flash AFCommerce Shopping Cart allows remote attackers to execute arbitrary SQL commands via the search field.	unknown 2006-07-24	7.0	CVE-2006-3794 BUGTRAQ BID XF
Darren's \$5 Script Archive -- osDate	Cross-site scripting (XSS) vulnerability in showprofile.php in Darren's \$5 Script Archive osDate 1.1.7 and earlier allows remote attackers to inject arbitrary web script or HTML via the onerror attribute in an HTML IMG tag with a non-existent source file in txtcomment parameter, which is used when posting a comment.	unknown 2006-07-21	7.0	CVE-2006-3767 BUGTRAQ BUGTRAQ BID FRSIRT SECUNIA
DeluxeBB -- DeluxeBB	DeluxeBB 1.07 and earlier does not properly handle a username composed of a single space character, which allows remote authenticated users to login as the "space" user, post as the guest user, and block the ability of an administrator to ban the "space" user.	unknown 2006-07-24	7.0	CVE-2006-3796 BUGTRAQ

DeluxeBB -- DeluxeBB	SQL injection vulnerability in DeluxeBB 1.07 and earlier allows remote attackers to bypass authentication, spoof users, and modify settings via the (1) memberpw and (2) membercookie cookies.	unknown 2006-07-24	7.0	CVE-2006-3797 BUGTRAQ
DeluxeBB -- DeluxeBB	DeluxeBB 1.07 and earlier allows remote attackers to bypass SQL injection protection mechanisms via the login variable and certain other variables, by using lowercase "union select" or possibly other statements that do not match the uppercase "UNION SELECT."	unknown 2006-07-24	7.0	CVE-2006-3799 BUGTRAQ BID FRSIRT SECUNIA
eIQnetworks -- Enterprise Security Analyzer	Multiple stack-based buffer overflows in eIQnetworks Enterprise Security Analyzer before 2.5.0 allow remote attackers to execute arbitrary code via long (1) DELTAINTERVAL, (2) LOGFOLDER, (3) DELETEDLOGS, (4) FWASERVER, (5) SYSLOGPUBLICIP, (6) GETFWAIMPORTLOG, (7) GETFWADELTA, (8) DELETERDEPDEVICE, (9) COMPRESSRAWLOGFILE, (10) GETSYSLOGFIREWALLS, (11) ADDPOLICY, and (12) EDITPOLICY commands to the (a) Syslog daemon (syslogserver.exe); (13) GUIADDDEVICE, (14) ADDDEVICE, and (15) DELETEDDEVICE commands to (b) the Topology server (Topology.exe); the LICMGR_ADDLICENSE command to the License Manager (EnterpriseSecurityAnalyzer.exe); and possibly other vectors related to the Syslog daemon (syslogserver.exe).	2006-05-10 2006-07-26	7.0	CVE-2006-3838 OTHER-REF OTHER-REF FRSIRT
Ethereal Group -- Ethereal Wireshark -- Wireshark	Multiple format string vulnerabilities in Wireshark (aka Ethereal) 0.10.x to 0.99.0 allow remote attackers to cause a denial of service and possibly execute arbitrary code via the (1) ANSI MAP, (2) Checkpoint FW-1, (3) MQ, (4) XML, and (5) NTP dissectors.	unknown 2006-07-21	7.0	CVE-2006-3628 WIRESHARK BUGTRAQ MANDRIVA BID FRSIRT SECUNIA SECUNIA GENTOO SECUNIA SECUNIA
Ethereal Group -- Ethereal	Multiple off-by-one errors in Wireshark (aka Ethereal) 0.9.7 to 0.99.0 have unknown impact and remote attack vectors via the (1) NCP	unknown 2006-07-21	7.0	CVE-2006-3630 WIRESHARK BUGTRAQ

	NMAS and (2) NDPS dissectors.			MANDRIVA BID FRSIRT SECUNIA SECUNIA GENTOO SECUNIA SECUNIA
Ethereal Group -- Ethereal	Buffer overflow in Wireshark (aka Ethereal) 0.8.16 to 0.99.0 allows remote attackers to cause a denial of service and possibly execute arbitrary code via the NFS dissector.	unknown 2006-07-21	7.0	CVE-2006-3632 WIRESHARK BUGTRAQ MANDRIVA BID FRSIRT SECUNIA SECUNIA GENTOO SECUNIA SECUNIA
Francisco Charrua -- Photo-Gallery	SQL injection vulnerability in Room.php in Francisco Charrua Photo-Gallery 1.0 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2006-07-21	7.0	CVE-2006-3688 BID FRSIRT SECUNIA BUGTRAQ SECTrack
Gerrit van Aaken -- Loudblog	SQL injection vulnerability in index.php in Gerrit van Aaken Loudblog 0.5 and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2006-07-25	7.0	CVE-2006-3832 BUGTRAQ OTHER-REF OTHER-REF FRSIRT SECUNIA
Gonafish -- LinksCaffe	Multiple SQL injection vulnerabilities in links.php in Gonafish LinksCaffe 3.0 allow remote attackers to execute arbitrary SQL commands via the (1) offset and (2) limit parameters, (3) newdays parameter in a new action, and the (4) link_id parameter in a deadlink action. NOTE: this issue can also be used for path disclosure by a forced SQL error, or to modify PHP files using OUTFILE.	unknown 2006-07-26	7.0	CVE-2006-3884 BUGTRAQ BID
Krusader -- Krusader	Krusader 1.50-beta1 up to 1.70.0 stores passwords for remote connections in cleartext in the bookmark file (krbookmarks.xml), which allows attackers to steal passwords by obtaining the file.	unknown 2006-07-25	7.0	CVE-2006-3816 OTHER-REF OTHER-REF
Mambo -- Mambo Calendar	PHP remote file inclusion vulnerability in com_calendar.php in Calendar Mambo Module 1.5.7 and earlier allows remote	unknown 2006-07-25	7.0	CVE-2006-3843 BUGTRAQ BID

	attackers to execute arbitrary PHP code via a URL in the absolute_path parameter.			
MusicBox -- MusicBox	SQL injection vulnerability in Shalwan MusicBox 2.3.4 and earlier allows remote attackers to execute arbitrary SQL commands via the page parameter in a viewgallery action in a request for the top-level URI. NOTE: the start parameter/search action is already covered by CVE-2006-1807, and the show parameter/top action is already covered by CVE-2006-1360.	unknown 2006-07-26	7.0	CVE-2006-3886 BUGTRAQ BID XF
MyBB -- MyBB	Cross-site scripting (XSS) vulnerability in inc/function_post.php in MyBB (aka MyBulletinBoard) 1.0 RC2 through 1.1.4 allows remote attackers to inject arbitrary web script or HTML via a javascript URI with an SGML numeric character reference in the url BBCode tag, as demonstrated using "javascript".	unknown 2006-07-21	7.0	CVE-2006-3761 BUGTRAQ OTHER-REF MYBB MYBB BID OSVDB SECUNIA XF
Oracle -- Oracle Database Server	Multiple unspecified vulnerabilities in Oracle Database 10.1.0.5 have unknown impact and attack vectors, aka Oracle Vuln# (1) DB01 for Change Data Capture (CDC) component and (2) DB03 for Data Pump Metadata API. NOTE: as of 20060719, Oracle has not disputed a claim by a reliable researcher that DB01 is related to multiple SQL injection vulnerabilities in SYS.DBMS_CDC_IMPDP using the (a) IMPORT_CHANGE_SET, (b) IMPORT_CHANGE_TABLE, (c) IMPORT_CHANGE_COLUMN, (d) IMPORT_SUBSCRIBER, (e) IMPORT_SUBSCRIBED_TABLE, (f) IMPORT_SUBSCRIBED_COLUMN, (g) VALIDATE_IMPORT, (h) VALIDATE_CHANGE_SET, (i) VALIDATE_CHANGE_TABLE, and (j) VALIDATE_SUBSCRIPTION procedures, and that DB03 is for SQL injection in the MAIN procedure for SYS.KUPW\$WORKER.	unknown 2006-07-21	7.0	CVE-2006-3698 OTHER-REF OTHER-REF BID FRSIRT BUGTRAQ BUGTRAQ OTHER-REF OTHER-REF CERT SECTrack SECUNIA HP FRSIRT SECUNIA XF
Pumpkin Studios -- Warzone Resurrection Pumpkin Studios -- Warzone	Stack-based buffer overflow in Warzone 2100 and Warzone Resurrection 2.0.3 and earlier allows remote attackers to execute arbitrary code via a (1) long message handled by the recvTextMessage function in multiplayer.c or a (2) long filename handled by NETrecvFile function in netplay/netplay.c.	unknown 2006-07-25	7.0	CVE-2006-3849 BUGTRAQ OTHER-REF BID FRSIRT XF XF

Silentweb -- ListMessenger	** DISPUTED ** PHP remote file inclusion vulnerability in enduser/listmessenger.php in ListMessenger 0.9.3 allows remote attackers to execute arbitrary PHP code via a URL in the lm_path parameter. NOTE: the vendor has disputed this issue to SecurityTracker, stating that the \$lm_path variable is set to a constant value. As of 20060726, CVE concurs with the vendor based on SecurityTracker's post-disclosure analysis.	unknown 2006-07-21	7.0	CVE-2006-3692 BUGTRAQ BID SECTRAK MLIST
Symantec -- pcAnywhere	Symantec pcAnywhere 12.5 uses weak default permissions for the "Symantec\pcAnywhere\Hosts" folder, which allows local users to gain privileges by inserting a superuser .cif (aka caller or CallerID) file into the folder, and then using a pcAnywhere client to login as a local administrator.	unknown 2006-07-24	7.0	CVE-2006-3784 BUGTRAQ OTHER-REF FRSIRT SECUNIA
Symantec -- pcAnywhere	Symantec pcAnywhere 12.5 obfuscates the passwords in a GUI textbox with asterisks but does not encrypt them in the associated .cif (aka caller or CallerID) file, which allows local users to obtain the passwords from the window using tools such as Nirsoft Asterwin.	unknown 2006-07-24	7.0	CVE-2006-3785 BUGTRAQ OTHER-REF
Symantec -- pcAnywhere	Symantec pcAnywhere 12.5 uses weak integrity protection for .cif (aka caller or CallerID) files, which allows local users to generate a custom .cif file and modify the superuser flag.	unknown 2006-07-24	7.0	CVE-2006-3786 BUGTRAQ OTHER-REF SECTRAK
TWiki -- TWiki	Eval injection vulnerability in the configure script in TWiki 4.0.0 through 4.0.4 allows remote attackers to execute arbitrary Perl code via an HTTP POST request containing a parameter name starting with "TYPEOF".	unknown 2006-07-26	7.0	CVE-2006-3819 OTHER-REF FRSIRT
UFO2000 -- UFO2000	Multiple buffer overflows in multiplay.cpp in UFO2000 svn 1057 allow remote attackers to execute arbitrary code via (1) a long unit name in Net::recv_add_unit,; (2) large values to Net::recv_rules, Net::recv_select_unit, Net::recv_options, and Net::recv_unit_data; and (3) a large mapdata GEODATA structure in Net::recv_map_data.	unknown 2006-07-24	7.0	CVE-2006-3788 BUGTRAQ OTHER-REF OTHER-REF OTHER-REF FRSIRT SECTRAK SECUNIA
UFO2000 -- UFO2000	Multiple array index errors in the (1) recv_rules, (2) recv_select_unit, (3) recv_options, and (4) recv_unit_data functions in multiplay.cpp in UFO2000 svn 1057 allow remote attackers to execute arbitrary code and cause a denial of service (opponent crash) via	unknown 2006-07-24	7.0	CVE-2006-3789 BUGTRAQ OTHER-REF OTHER-REF FRSIRT SECTRAK

	certain packet data that specifies an out-of-bounds index.			SECUNIA
UFO2000 -- UFO2000	SQL injection vulnerability in ServerClientUfo::recv_packet in server_protocol.cpp in UFO2000 svn 1057 allows remote attackers to execute arbitrary SQL commands via unspecified vectors involving the packet.c_str function.	unknown 2006-07-24	7.0	CVE-2006-3792 BUGTRAQ OTHER-REF OTHER-REF FRSIRT SECTrack SECUNIA
X7 Group -- X7 Chat	SQL injection vulnerability in upgradev1.php in X7 Chat 2.0.4 and earlier allows remote attackers to execute arbitrary SQL commands via the old_prefix parameter.	unknown 2006-07-25	7.0	CVE-2006-3851 OTHER-REF BID FRSIRT

[Back to top](#)

Medium Vulnerabilities				
Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
CaneBluem -- MoSpray	PHP remote file inclusion vulnerability in components/com_mospray/scripts/admin.php in MoSpray 1.8 RC1 allows remote attackers to execute arbitrary PHP code via a URL in the basedir parameter.	2006-07-23 2006-07-25	5.6	CVE-2006-3847 OTHER-REF OTHER-REF FRSIRT SECUNIA
Cheese Tracker -- Cheese Tracker	Buffer overflow in the Loader_XM::load_instrument_internal function in loader_xm.cpp for Cheese Tracker 0.9.9 and earlier allows user-assisted attackers to execute arbitrary code via a crafted file with a large amount of extra data.	unknown 2006-07-25	4.7	CVE-2006-3814 OTHER-REF BUGTRAQ BID
fbi -- fbi	The fbgs framebuffer Postscript/PDF viewer in fbi before 2.01 has a typo that prevents a filter from working correctly, which allows user-assisted attackers to bypass the filter and execute malicious Postscript commands.	unknown 2006-07-25	5.6	CVE-2006-3119 DEBIAN
GeodesicSolutions -- GeoAuctions Enterprise	SQL injection vulnerability in index.php in GeodesicSolutions GeoAuctions Enterprise 1.0.6 allows remote attackers to execute arbitrary SQL commands via the d parameter.	unknown 2006-07-25	5.6	CVE-2006-3822 OTHER-REF BID
GeodesicSolutions -- GeoClassifieds Basic GeodesicSolutions -- GeoAuctions Premier	SQL injection vulnerability in index.php in GeodesicSolutions (1) GeoAuctions Premier 2.0.3 and (2) GeoClassifieds Basic 2.0.3 allows remote attackers to execute arbitrary SQL commands via the b parameter.	unknown 2006-07-25	5.6	CVE-2006-3823 OTHER-REF BID

Gerrit van Aaken -- Loudblog	Cross-site scripting (XSS) vulnerability in loudblog/index.php in Loudblog before 0.5 allows remote attackers to inject arbitrary web script or HTML via the page parameter.	unknown 2006-07-25	4.7	CVE-2006-3820 OTHER-REF OTHER-REF BID FRSIRT SECUNIA XF
Kailash Nadh -- boastMachine	SQL injection vulnerability in bmc/Inc/core/admin/search.inc.php in Kailash Nadh boastMachine (formerly bMachine) 3.1 and earlier allows remote authenticated administrators to execute arbitrary SQL commands via the blog parameter.	unknown 2006-07-25	4.2	CVE-2006-3827 BUGTRAQ OTHER-REF FRSIRT SECTrack SECUNIA
Kailash Nadh -- boastMachine	Incomplete blacklist vulnerability in Kailash Nadh boastMachine (formerly bMachine) 3.1 and earlier allows remote authenticated administrators to bypass SQL injection protection mechanisms by using commas, quote characters, pound sign (#) characters, "UNION," and "SELECT," which are not filtered by the product, which only checks for "insert," "delete," "update," and "replace."	unknown 2006-07-25	4.2	CVE-2006-3828 BUGTRAQ OTHER-REF FRSIRT SECTrack SECUNIA
Lussumo -- Vanilla	** DISPUTED ** PHP remote file inclusion vulnerability in upgrader.php in Vanilla CMS 1.0.1 and earlier, when /conf/old_settings.php exists, allows remote attackers to execute arbitrary PHP code via a URL in the RootDirectory parameter. NOTE: this issue has been disputed by a third party who states that the RootDirectory parameter is initialized before being used, for version 1.0. CVE analysis concurs with the dispute, but it is unclear whether older versions are affected.	unknown 2006-07-25	5.6	CVE-2006-3850 BUGTRAQ MLIST MLIST BID
Mambo -- Mambo MultiBanners	PHP remote file inclusion vulnerability in extadminmenus.class.php in the MultiBanners 1.0.1 for Mambo allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter.	unknown 2006-07-25	5.6	CVE-2006-3846 BUGTRAQ OTHER-REF FRSIRT SECUNIA
Oracle -- Oracle Database Server	Multiple unspecified vulnerabilities in Oracle Database 8.1.7.4, 9.0.1.5, 9.2.0.7, 10.1.0.5, and 10.2.0.2 have unknown impact and attack vectors, aka Oracle Vuln# (1) DB06 in Export; (2) DB08, (3) DB09, (4) DB10, (5) DB11, (6) DB12, (7) DB13, (8) DB14, and (9) DBC01 for OCI; (10) DB16 for Query Rewrite/Summary Mgmt; (11) DB17, (12) DB18, (13) DB19, (14) DBC02, (15) DBC03, and (16) DBC04 for RPC; and (17) DB20 for	unknown 2006-07-21	4.9	CVE-2006-3702 OTHER-REF OTHER-REF BID FRSIRT OTHER-REF CERT CERT-VN SECTrack SECUNIA

	Semantic Analysis. NOTE: as of 20060719, Oracle has not disputed third party claims that DB06 is related to "SQL injection" using DBMS_EXPORT_EXTENSION with a modified ODCIIndexGetMetadata routine and a call to GET_DOMAIN_INDEX_METADATA, in which case DB06 might be CVE-2006-2081.			HP FRSIRT SECUNIA
Oracle -- Oracle Database Server	Multiple unspecified vulnerabilities in Oracle Database 10.1.0.5 have unknown impact and attack vectors, aka Oracle Vuln# (1) DB21 for Statistics and (2) DB22 for Upgrade & Downgrade. NOTE: as of 20060719, Oracle has not disputed a claim by a reliable researcher that DB21 is for a local SQL injection vulnerability in SYS.DBMS_STATS, and that DB22 is for SQL injection in SYS.DBMS_UPGRADE.	unknown 2006-07-21	4.9	CVE-2006-3705 OTHER-REF OTHER-REF BID FRSIRT BUGTRAQ BUGTRAQ OTHER-REF OTHER-REF CERT SECTrack SECUNIA HP FRSIRT SECUNIA
OSSP -- shiela	OSSP shiela 1.1.5 and earlier allows remote authenticated users to execute arbitrary commands on the CVE server via shell metacharacters in a filename that is committed.	unknown 2006-07-26	4.2	CVE-2006-3633 OTHER-REF OPENPKG FRSIRT
Pablo Software Solutions -- Quick 'n Easy FTP Server	Buffer overflow in Quick 'n Easy FTP Server 3.0 allows remote authenticated users to execute arbitrary commands via a long argument to the LIST command, a different issue than CVE-2006-2027.	unknown 2006-07-25	4.2	CVE-2006-3844 OTHER-REF BID SECUNIA
RARLAB -- WinRAR	Stack-based buffer overflow in lzh.fmt in WinRAR 3.00 through 3.60 beta 6 allows remote attackers to execute arbitrary code via a long filename in a LHA archive.	unknown 2006-07-25	5.6	CVE-2006-3845 OTHER-REF OTHER-REF FRSIRT SECUNIA XF
SiteDepth -- SiteDepth CMS	PHP remote file inclusion vulnerability in constants.php in SiteDepth CMS 3.01 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the SD_DIR parameter.	unknown 2006-07-24	5.6	CVE-2006-3793 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA XF

[Back to top](#)

Low Vulnerabilities				
Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
3Com -- TippingPoint IPS	TippingPoint IPS running the TippingPoint Operating System (TOS) before 2.2.4.6519 allows remote attackers to "force the device into layer 2 fallback (L2FB)", causing a denial of service (page fault), via a malformed packet.	2005-06-02 2006-07-26	2.3	CVE-2006-3678 BUGTRAQ OTHER-REF BID FRSIRT
AdventNet -- Zoho Virtual Office	Cross-site scripting (XSS) vulnerability in Zoho Virtual Office 3.2 Build 3210 allows remote attackers to execute arbitrary web script or HTML via an HTML message.	unknown 2006-07-25	2.3	CVE-2006-3842 BUGTRAQ BID SECUNIA
Amazing Flash Commerce -- AFCommerce Shopping Cart	Cross-site scripting (XSS) vulnerability in Amazing Flash AFCommerce Shopping Cart allows remote attackers to inject arbitrary web script or HTML via the "new review" text box.	unknown 2006-07-24	2.3	CVE-2006-3800 BUGTRAQ BID XF
Apache Group -- Tomcat	Apache Tomcat 5 before 5.5.17 allows remote attackers to list directories via a semicolon (;) preceding a filename with a mapped extension, as demonstrated by URLs ending with /;index.jsp and /;help.do.	unknown 2006-07-25	2.3	CVE-2006-3835 FULLDISC BID XF
ATutor -- ATutor	Multiple cross-site scripting (XSS) vulnerabilities in ATutor 1.5.3 allow remote attackers to inject arbitrary web script or HTML via the (1) lang parameter in (a) index_list.php and (2) year, (3) month, and (4) day parameter in (b) registration.php.	unknown 2006-07-25	2.3	CVE-2006-3821 BUGTRAQ BUGTRAQ
Check Point Software -- Check Point FireWall-1	Directory traversal vulnerability in Check Point Firewall-1 R55W before HFA03 allows remote attackers to read arbitrary files via an encoded .. (dot dot) in the URL on TCP port 18264.	unknown 2006-07-26	2.3	CVE-2006-3885 BUGTRAQ OTHER-REF BID FRSIRT XF
DeluxeBB -- DeluxeBB	Multiple cross-site scripting (XSS) vulnerabilities in DeluxeBB before 1.08 allow remote attackers to inject arbitrary web script or HTML via the (1) membercookie cookie in header.php and the (2) redirect parameter in misc.php.	unknown 2006-07-24	1.9	CVE-2006-3795 BUGTRAQ BID FRSIRT SECUNIA XF XF
DeluxeBB -- DeluxeBB	DeluxeBB 1.07 and earlier allows remote attackers to overwrite the (1) _GET, (2) _POST, (3) _ENV, and (4) _SERVER variables via the _COOKIE (aka COOKIE)	unknown 2006-07-24	2.3	CVE-2006-3798 BUGTRAQ

	variable, which can overwrite the other variables during an extract function call, probably leading to multiple security vulnerabilities, aka "pollution of the global namespace."			
EJ3 Soft -- TOPo	index.php in EJ3 TOPo 2.2.178 allows remote attackers to overwrite existing entries and establish new passwords for the overwritten entries via a URL with a modified entry ID.	unknown 2006-07-25	2.3	CVE-2006-3833 BUGTRAQ
EJ3 Soft -- TOPo	EJ3 TOPo 2.2.178 includes the password in cleartext in the ID field to index.php, which allows context-dependent attackers to obtain entry passwords via log files, referrers, or other vectors.	unknown 2006-07-25	2.3	CVE-2006-3834 BUGTRAQ
Ethereal Group -- Ethereal Wireshark -- Wireshark	Unspecified vulnerability in the GSM BSSMAP dissector in Wireshark (aka Ethereal) 0.10.11 to 0.99.0 allows remote attackers to cause a denial of service (crash) via unspecified vectors.	unknown 2006-07-21	3.3	CVE-2006-3627 WIRESHARK BUGTRAQ MANDRIVA BID FRSIRT SECUNIA SECUNIA GENTOO SECUNIA SECUNIA
Ethereal Group -- Ethereal	Unspecified vulnerability in the MOUNT dissector in Wireshark (aka Ethereal) 0.9.4 to 0.99.0 allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors.	unknown 2006-07-21	2.3	CVE-2006-3629 WIRESHARK BUGTRAQ MANDRIVA BID FRSIRT SECUNIA SECUNIA GENTOO SECUNIA SECUNIA
Ethereal Group -- Ethereal	Unspecified vulnerability in the SSH dissector in Wireshark (aka Ethereal) 0.9.10 to 0.99.0 allows remote attackers to cause a denial of service (infinite loop) via unknown attack vectors.	unknown 2006-07-21	3.3	CVE-2006-3631 WIRESHARK BUGTRAQ MANDRIVA BID FRSIRT SECUNIA SECUNIA GENTOO SECUNIA SECUNIA

FastJar -- FastJar	Directory traversal vulnerability in FastJar 0.93, as used in Gnu GCC 4.1.1 and earlier, and 3.4.6 and earlier, allows user-assisted attackers to overwrite arbitrary files via a .jar file containing filenames with "../" sequences.	unknown 2006-07-25	1.9	CVE-2006-3619 OTHER-REF OTHER-REF BID FRSIRT FRSIRT OSVDB SECUNIA SECUNIA
Gonafish -- LinksCaffe	Multiple cross-site scripting (XSS) vulnerabilities in Gonafish LinksCaffe 3.0 allow remote attackers to inject arbitrary web script or HTML via (1) the tablewidth parameter in (a) counter.php; (2) the newdays parameter in (b) links.php; and the (3) tableborder, (4) menucolor, (5) textcolor, and (6) bodycolor parameters in (c) menu.inc.php.	unknown 2006-07-26	2.3	CVE-2006-3883 BUGTRAQ BID
ISS -- RealSecure Desktop ISS -- RealSecure Network ISS -- BlackICE Server Protection ISS -- BlackICE PC Protection ISS -- RealSecure Server Sensor ISS -- Proventia Server ISS -- Proventia Desktop ISS -- Proventia	The SMB Mailslot parsing functionality in PAM in multiple ISS products with XPU (24.39/1.78/epj/x.x.x.1780), including Proventia A, G, M, Server, and Desktop, BlackICE PC and Server Protection 3.6, and RealSecure 7.0, allows remote attackers to cause a denial of service (infinite loop) via a crafted SMB packet that is not properly handled by the SMB_Mailslot_Heap_Overflow decode.	unknown 2006-07-27	1.9	CVE-2006-3840 OTHER-REF FRSIRT ISS
Kailash Nadh -- boastMachine	Multiple cross-site scripting (XSS) vulnerabilities in Kailash Nadh boastMachine (formerly bMachine) 3.1 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) user_login, (2) full_name, and (3) URL parameters in register.php; and allow remote authenticated administrators to inject arbitrary web script or HTML via the (4) cat_list and (5) key parameters in a certain portion of the admin interface.	unknown 2006-07-25	2.3	CVE-2006-3826 BUGTRAQ OTHER-REF FRSIRT SECTrack SECUNIA
Kailash Nadh -- boastMachine	Cross-site request forgery (CSRF) vulnerability in bmc/admin.php in Kailash Nadh boastMachine (formerly bMachine) 3.1 and earlier allows remote attackers to perform unauthorized actions as an administrator and delete arbitrary user accounts via a delete_user	unknown 2006-07-25	2.3	CVE-2006-3829 BUGTRAQ OTHER-REF SECTrack SECUNIA

	action.			
Kailash Nadh -- boastMachine	The Languages selection in the admin interface in Kailash Nadh boastMachine (formerly bMachine) 3.1 and earlier allows remote authenticated administrators to upload files with arbitrary extensions to the bmc/Inc/Lang directory. NOTE: because the uploaded files cannot be accessed through HTTP, this issue is a vulnerability only if there is a likely usage pattern in which the files would be opened or executed by local users, e.g., malware files with names that entice local users to open the files.	unknown 2006-07-25	1.4	CVE-2006-3830 OTHER-REF SECUNIA
Kailash Nadh -- boastMachine	The Backup selection in Kailash Nadh boastMachine (formerly bMachine) 3.1 and earlier uses predicable filenames for database backups and stores the files under the web root with insufficient access control, which allows remote attackers to obtain sensitive information by downloading a backup file.	unknown 2006-07-25	2.3	CVE-2006-3831 BUGTRAQ OTHER-REF SECTRAK SECUNIA
Krischan Jodies -- IP Calculator	Cross-site scripting (XSS) vulnerability in CGI wrapper for IP Calculator (IPCalc) 0.40 allows remote attackers to inject arbitrary web script or HTML via the URI (REQUEST_URI environment variable), which is used in the actionurl variable.	unknown 2006-07-25	1.9	CVE-2006-3848 FULLDISC OTHER-REF FRSIRT OSVDB SECUNIA
Linux-HA -- heartbeat	heartbeat.c in heartbeat before 2.0.6 sets insecure permissions in a shmget call for shared memory, which allows local users to cause an unspecified denial of service via unknown vectors, possibly during a short time window on startup.	unknown 2006-07-25	1.6	CVE-2006-3815 OTHER-REF OTHER-REF
Microsoft -- Windows 2000 Microsoft -- Windows Server 2003 Microsoft -- Windows XP	** DISPUTED ** Microsoft Windows NT 4.0, Windows 2000, Windows XP, and Windows Small Business Server 2003 allow remote attackers to cause a denial of service (IP stack hang) via a continuous stream of packets on TCP port 135 that have incorrect TCP header checksums and random numbers in certain TCP header fields, as demonstrated by the Achilles Windows Attack Tool. NOTE: the researcher reports that the Microsoft Security Response Center has stated "Our investigation which has included code review, review of the TCPCDump, and attempts on reproing the issue on multiple fresh installs of various Windows Operating Systems have all resulted in non confirmation."	unknown 2006-07-26	2.3	CVE-2006-3880 BUGTRAQ BID

Microsoft -- Internet Explorer	Stack overflow in Microsoft Internet Explorer 6 on Windows 2000 allows remote attackers to cause a denial of service (application crash) by creating an NMSA.ASFSourceMediaDescription.1 ActiveX object with a long dispValue property.	unknown 2006-07-27	2.3	CVE-2006-3897 OTHER-REF BID FRSIRT OSVDB XF
Miod Vallat -- mikmod	Integer overflow in the loadChunk function in loaders/load_gt2.c in libmikmod in Mikmod Sound System 3 through 3.2.2 allows remote attackers to cause a denial of service via a GRAOUMF TRACKER (GT2) module file with a large (0xFFFFFFFF) comment length value in an XCOM chunk.	unknown 2006-07-26	2.3	CVE-2006-3879 BUGTRAQ OTHER-REF BID
MusicBox -- MusicBox	Cross-site scripting (XSS) vulnerability in Shalwan MusicBox 2.3.4 and earlier allows remote attackers to inject arbitrary web script or HTML via the id parameter in a request for the top-level URI. NOTE: the id parameter in index.php, and the type and show parameters in a top action, are already covered by CVE-2006-1349; and the term parameter in a search action is already covered by CVE-2006-1806.	unknown 2006-07-26	2.3	CVE-2006-3881 BUGTRAQ XF
MusicBox -- MusicBox	Shalwan MusicBox 2.3.4 and earlier allows remote attackers to obtain configuration information via a direct request to phpinfo.php, which calls the phpinfo function.	unknown 2006-07-26	2.3	CVE-2006-3882 BUGTRAQ
Opware -- Network Automation System	Opware Network Automation System (NAS) 6.0 installs /etc/init.d/mysql with world-readable permissions, which allows local users to read the root password for the MySQL MAX database.	unknown 2006-07-26	1.6	CVE-2006-3878 BUGTRAQ BID SECTRACK
OWASP -- WebScarab	Cross-site scripting (XSS) vulnerability in WebScarab before 20060718-1904, when used with Microsoft Internet Explorer 6 SP2 or Konqueror 3.5.3, allows remote attackers to inject arbitrary web script or HTML via the URL, which is not sanitized before being returned in an error message when WebScarab is not able to access the URL.	unknown 2006-07-25	1.9	CVE-2006-3841 BUGTRAQ OTHER-REF SECUNIA
PHPTOys -- Micro Guestbook	Cross-site scripting (XSS) vulnerability in index.php in Micro GuestBook allows remote attackers to execute arbitrary SQL commands via the (1) name or (2) comment ("text") fields.	2006-07-22 2006-07-25	2.3	CVE-2006-3852 BUGTRAQ

Professional Home Page Tools -- Guestbook	delcookie.php in Professional Home Page Tools Guestbook changes the expiration date of a cookie instead of deleting the cookie's value, which makes it easier for attackers to steal the cookie and obtain the administrator's password hash after logout.	unknown 2006-07-25	2.3	CVE-2006-3837 BUGTRAQ OTHER-REF SECUNIA XF
Sun -- Solaris	Unspecified vulnerability in the kernel in Solaris 10 with patch 118822-29 (118844-29 on x86) and without patch 118833-11 (118855-08) allows remote authenticated users to cause a denial of service via unspecified vectors that lead to "kernel data structure corruption" that can trigger a system panic, application failure, or "data corruption."	unknown 2006-07-21	2.0	CVE-2006-3728 SUNALERT BID FRSIRT SECUNIA XF SECTrack
Sun -- Solaris	Sun Solaris 10 allows local users to cause a denial of service (panic) via unspecified vectors involving (1) the /net mount point and (2) the "-hosts" map in a mount point.	unknown 2006-07-24	1.6	CVE-2006-3783 SUNALERT FRSIRT BID SECTrack SECUNIA XF
Sun -- Solaris	systeminfo.c for Sun Solaris allows local users to read kernel memory via a 0 variable count argument to the sysinfo system call, which causes a -1 argument to be used by the copyout function. NOTE: this issue has been referred to as an integer overflow, but it is probably more like a signedness error or integer underflow.	unknown 2006-07-25	2.3	CVE-2006-3824 IDEFENSE BID
Sun -- Solaris	The IPv4 implementation in Sun Solaris 10 before 20060721 allows local users to select routes that differ from the routing table, possibly facilitating firewall bypass or unauthorized network communication.	unknown 2006-07-25	1.6	CVE-2006-3825 SUNALERT BID FRSIRT SECUNIA XF
Sunbelt Software -- Kerio Personal Firewall	kpf4ss.exe in Sunbelt Kerio Personal Firewall 4.3.x before 4.3.268 does not properly hook the CreateRemoteThread API function, which allows local users to cause a denial of service (crash) and bypass protection mechanisms by calling CreateRemoteThread.	unknown 2006-07-24	1.6	CVE-2006-3787 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA
UFO2000 -- UFO2000	The decode_stringmap function in server_transport.cpp for UFO2000 svn 1057 allows remote attackers to cause a denial of service (daemon termination) via a keysize or valsize that is inconsistent with the packet size, which leads to a buffer over-read.	unknown 2006-07-24	2.3	CVE-2006-3790 BUGTRAQ OTHER-REF OTHER-REF FRSIRT SECTrack SECUNIA

UFO2000 -- UFO2000	The decode_stringmap function in server_transport.cpp for UFO2000 svn 1057 allows remote attackers to cause a denial of service (daemon termination) via a large keysize or valsize, which causes a crash when the resize function cannot allocate sufficient memory.	unknown 2006-07-24	2.3	CVE-2006-3791 BUGTRAQ OTHER-REF OTHER-REF FRSIRT SECTrack SECUNIA
UNIDOMedia -- Chameleon LE	Directory traversal vulnerability in index.php in UNIDOMedia Chameleon LE 1.203 and earlier, and possibly Chameleon PRO, allows remote attackers to read arbitrary files via the rmid parameter.	unknown 2006-07-25	2.3	CVE-2006-3836 BUGTRAQ BID

[Back to top](#)

Last updated July 31, 2006